Are You the Weakest Link?

Human Error in Cyber Security and How to Fix It.

Cyber security remains a critical concern for New Zealand businesses of all sizes. Despite significant investments in security technology, human error remains one of the largest vulnerabilities. This article explores how human mistakes, including social engineering and poor password hygiene, compromise security, and outlines practical steps Kiwi companies can take to address these risks.

Understanding the Risk: Why Human Error Matters

Human error is responsible for over 90% of cybersecurity breaches. In New Zealand, CERT NZ reported a marked increase in cyber incidents in recent years, with phishing scams, business email compromises (BEC), and social engineering ranking among the most prevalent.

Common human errors include:

- Clicking malicious links or attachments.
- Weak or reused passwords.
- Failure to report suspicious activities promptly.

Social Engineering: Manipulating Trust

Social engineering attacks exploit human psychology, manipulating staff to gain confidential information or system access.

Types of Social Engineering:

- **Phishing Emails:** Carefully designed emails mimicking trusted sources.
- **Vishing (Voice Phishing):** Calls from attackers posing as legitimate personnel.
- **Smishing (SMS Phishing):** Deceptive text messages urging immediate action.

Real-world Case: NZ Businesses Targeted

An Auckland business lost over NZD 150,000 due to a sophisticated phishing email mimicking a supplier's legitimate invoice request. The employee, unaware of the deception, facilitated a fraudulent bank transfer.

Password Hygiene: The Simplest Defence Often Neglected

Poor password management remains a significant vulnerability in many New Zealand businesses. Despite awareness campaigns, many employees still use easily guessable or repeatedly reused passwords across multiple accounts.

Best Practices for Password Security:

- **Implement Multi-Factor Authentication (MFA):** Adds an additional security layer.
- **Use Password Managers:** Automates secure password generation and storage.
- **Regular Updates and Complexity Requirements:** Mandate periodic password changes with strong complexity standards.

How New Zealand Companies Are Responding

Leading Kiwi companies increasingly focus on staff training and cyber awareness programs to strengthen their security posture.

Key Strategies Include:

- **Regular Staff Training:** Interactive sessions and microlearning modules.
- **Simulated Phishing Attacks:** Identify vulnerability and educate staff effectively.
- **Clear Reporting Protocols:** Ensure employees know how and when to report suspicious activity.
- **Embedding Cybersecurity Culture:** Making security awareness part of everyday operations.

Success Story: Upskilling with Aspire2 Education

New Zealand businesses partner with education providers such as Aspire2 Education to deliver NZQA-approved online IT courses, including modules on technical support and security. These programmes help employees develop skills to protect systems, maintain data integrity, and respond effectively to potential threats, significantly reducing organisational risk.

Practical Steps to Minimise Human Error in Your Organisation

1. **Leadership Commitment:** Cyber security must be championed by senior management.
2. **Continuous Education:** Invest in regular and engaging cybersecurity training.
3. **Implement and Enforce Policies:** Strong policies around password management, incident reporting, and safe digital behaviour.
4. **Reward Positive Behaviour:** Encourage and reward staff who demonstrate strong cybersecurity awareness and initiative.
5. **Leverage Technology:** Utilise advanced solutions such as MFA and automated threat detection tools.

Conclusion: Transforming Human Error into Human Defence

In the digital age, cybersecurity is a shared responsibility. While human error can introduce vulnerabilities, informed and well-trained staff can significantly strengthen an organisation's defences. By investing in education, fostering a culture of security awareness, and promoting consistent best practices, New Zealand businesses can turn their teams into one of their strongest assets in protecting against digital threats.

To learn more about how Aspire2 Education's IT programmes can help you and your team strengthen it's digital defences, explore our course offerings.